



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,476	08/13/2001	Luu Tran	SUN-P6088	9070

32615 7590 04/28/2006

OSHA LIANG L.L.P./SUN
1221 MCKINNEY, SUITE 2800
HOUSTON, TX 77010

EXAMINER

POPHAM, JEFFREY D

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 04/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/929,476

Applicant(s)

TRAN ET AL.

Examiner

Jeffrey D. Popham

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 April 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5 and 7-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5 and 7-27 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 13 April 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Remarks

Claims 1-5 and 7-27 are pending.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/5/2006 has been entered.

Response to Arguments

2. Applicant's arguments filed 4/5/2006 have been fully considered but they are not persuasive. Applicant argues that Lloyd fails to disclose or suggest using unique authentication parameters, such as the wireless client's browser type, operating system, etc. to authenticate each client in a class of wireless clients. In Lloyd, however, the choice of which authentication mechanism is to be used for a particular client is dependent upon which operating system the client is running (clients communicate with the authentication server in their native protocol). This can be seen in that authentication requests include the operating system type that the client is running (Column 7, lines 56-67). Column 11, line 55 to Column 12, line 4 discuss authentication mechanisms such as cryptographic authentication devices and how a particular

Art Unit: 2137.

authentication mechanism will only be available to a particular client if the server determines that the client is capable of supporting such a mechanism. It also describes how the service could be specific to a certain authentication mechanism, such that a user ID and password could get access to some data, but not all, while using a cryptographic authentication device would grant access to more data. As can be seen, the authentication mechanism used within Lloyd is dependent at least upon the client OS, the client's capabilities (for supporting a given authentication mechanism), and the service/data to which access is requested.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-5, 7, 8, 15-18, and 24-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Lloyd (U.S. Patent 6,219,790).

Regarding Claim 1,

Lloyd discloses a client aware authentication system in a wireless network (Column 13, line 61 to Column 14, line 8; whenever wireless is

referred to as being within Lloyd, reference is made to this paragraph),
comprising:

A wireless server (Column 4, lines 22-29);

A plurality of classes of wireless clients, each of the plurality of
classes of wireless clients having unique authentication parameters
(Column 1, line 66 to Column 2, line 28; Column 6, lines 34-40; Column
11, line 55 to Column 12, line 4; and Figure 2); and

A plurality of authentication modules, wherein the plurality of
authentication modules selectively provide client specific authentication
information to authenticate each of the plurality of classes of wireless
clients using the unique authentication parameters (Column 1, line 66 to
Column 2, line 28; Column 6, line 34 to Column 7, line 10; Column 11, line
55 to Column 12, line 4; and Figure 2),

Wherein the unique authentication parameters comprises at least
one selected from the group consisting of a browser type executing on the
wireless client, a type of operating system executing on the wireless client,
a version of the browser executing on the wireless client, and a bandwidth
of the wireless client (Column 1, line 66 to Column 2, line 28; and Column
6, line 34 to Column 7, line 23).

Regarding Claim 2,

Lloyd discloses that the plurality of authentication modules are
coupled to an authentication service and wherein the authentication

service is for dynamically selecting an authentication service module based on the class of a client (Column 6, line 34 to Column 7, line 23; and Column 11, line 55 to Column 12, line 4).

Regarding Claim 3,

Lloyd discloses that the authentication service receives and parses client type information of the wireless clients to determine authentication characteristics of the wireless clients (Column 7, lines 41-45).

Regarding Claim 4,

Lloyd discloses that the plurality of authentication modules comprises a set of predefined authentication parameters used by the wireless server to authenticate the wireless clients with known authentication characteristics accessing the wireless server (Column 6, line 34 to Column 7, line 23; and Column 11, line 55 to Column 12, line 4).

Regarding Claim 5,

Lloyd discloses that the plurality of authentication modules further comprises authentication parameters dynamically extracted from client type information of the wireless clients accessing the wireless server (Column 7, lines 56-67).

Regarding Claim 7,

Lloyd discloses a wireless server system, comprising:

A plurality of authentication modules each providing respective authentication parameters pertinent to a type of client, wherein the unique

Art Unit: 2137

authentication parameters are used to authenticate each of the plurality of wireless clients (Column 1, line 66 to Column 2, line 28; Column 6, line 34 to Column 7, line 10; Column 11, line 55 to Column 12, line 4; and Figure 2); and

An authentication service, in response to receiving a particular client type associated with a particular wireless device, for dynamically selecting an authentication module of the plurality of authentication modules based on the particular client type (Column 1, line 66 to Column 2, line 28; Column 6, line 34 to Column 7, line 10; Column 11, line 55 to Column 12, line 4; and Figure 2),

Wherein the type of client is determined using at least one selected from the group consisting of a browser type executing on the wireless device, a type of operating system executing on the wireless device, a version of the browser executing on the wireless device, and a bandwidth of the wireless device (Column 1, line 66 to Column 2, line 28; and Column 6, line 34 to Column 7, line 23); and

Wherein the authentication service is also for applying a selected authentication module to the particular wireless device for the authentication thereof (Column 1, line 66 to Column 2, line 28; and Column 6, line 34 to Column 7, line 10; Column 11, line 55 to Column 12, line 4).

Regarding Claim 8,

Lloyd discloses an automatic client detection service for automatically detecting the particular client type in response to service requests that originate from the particular wireless device (Column 7, lines 56-67).

Regarding Claim 15,

Lloyd discloses a wireless server, comprising:

A client aware authentication service logic (Column 6, lines 34-40);

A plurality of client aware authentication modules, wherein the plurality of client aware authentication modules selectively provide client specific authentication information to authenticate each of a plurality of wireless clients using unique authentication parameters (Column 1, line 66 to Column 2, line 28; Column 6, line 34 to Column 7, line 10; Column 11, line 55 to Column 12, line 4; and Figure 2),

Wherein the unique authentication parameters comprise at least one selected from the group consisting of a browser type executing on the wireless client, a type of operating system executing on the wireless client, a version of the browser executing on the wireless client, and a bandwidth of the wireless client (Column 1, line 66 to Column 2, line 28; and Column 6, line 34 to Column 7, line 23);

A client data storage module for storing client type information (Column 4, lines 22-47); and

A session service module for storing transient session information for a client requesting authentication to the wireless server (Column 13, lines 1-21).

Regarding Claim 16,

Lloyd discloses that the authentication service logic authenticates client attempting to access the wireless server (Column 6, line 34 to Column 7, line 23).

Regarding Claim 17,

Lloyd discloses that the authentication service logic retrieves client type information from the client data storage module and stores the client type information in the session service module to enable the client to be authenticated by the wireless server (Column 6, line 34 to Column 7, line 23; and Column 13, lines 1-21).

Regarding Claim 18,

Lloyd discloses that the authentication modules comprise a set of predefined authentication parameters for authenticating known classes of wireless clients that access the wireless server (Column 6, line 34 to Column 7, line 23).

Regarding Claim 24,

Lloyd discloses a client aware authentication module, comprising:

A plurality of client aware characteristics modules, wherein the plurality of client aware characteristics modules provide client specific

authentication information in order to authenticate a plurality of wireless clients accessing a wireless server (Column 1, line 66 to Column 2, line 28; Column 6, line 34 to Column 7, line 10; Column 11, line 55 to Column 12, line 4; and Figure 2),

Wherein the client aware authentication module uses unique identification parameters associated with each of the plurality of wireless clients to authenticate each of the plurality of wireless clients and determine which of the plurality of client aware characteristics modules to use (Column 1, line 66 to Column 2, line 28; Column 6, line 34 to Column 7, line 10; Column 11, line 55 to Column 12, line 4; and Figure 2),

Wherein the unique identification parameters comprise at least one selected from the group consisting of a browser type, a type of operating system, a version of the browser, and a bandwidth (Column 1, line 66 to Column 2, line 28; and Column 6, line 34 to Column 7, line 23); and

Client aware authentication selection logic (Column 6, line 34 to Column 7, line 23; and Column 11, line 55 to Column 12, line 4).

Regarding Claim 25,

Lloyd discloses that the plurality of client aware characteristics modules comprise predefined set of client characteristics for authenticating known clients accessing the client aware authentication modules (Column 6, line 34 to Column 7, line 23; and Column 11, line 55 to Column 12, line 4).

Regarding Claim 26,

Lloyd discloses that the plurality of client aware characteristics modules comprise client characteristics dynamically extracted from the client run-time environment (Column 7, lines 56-67).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 9-12 and 19-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lloyd in view of Liao (U.S. Patent 6,606,663).

Regarding Claim 9,

Lloyd discloses that the service requests comprise information which is used to detect the particular client type (Column 7, lines 56-67), but does not disclose that this information is header information.

Liao, however, discloses that the service requests comprise header information, including information about the particular client (Column 2, lines 18-35; and Column 7, lines 7-61). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the wireless system headers of Liao into the authentication system of Lloyd in order to reduce the number of bits and bytes that must be

transmitted over low bandwidth communication lines and to reduce the amount of memory used to store authentication information within each wireless client device (Column 2, lines 45-63).

Regarding Claim 10,

Lloyd as modified by Liao discloses the system of claim 9, in addition, Liao discloses that the header information comprises HTTP request headers (Column 2, lines 18-35; and Column 7, lines 7-61).

Regarding Claim 11,

Lloyd as modified by Liao discloses the system of claim 10, in addition, Lloyd discloses programmable user specific information within the authentication information transmitted to the server (Column 7, lines 56-67), and Liao discloses that the authentication information is transmitted in an authentication credential stored within the headers (Column 2, lines 18-35; and Column 7, lines 7-61).

Regarding Claim 12,

Lloyd as modified by Liao discloses the system of claim 11, in addition, Lloyd discloses that the authentication information comprises equipment manufacturer specified information (Column 11, lines 55-64), and Liao discloses that the authentication information is transmitted to the server in an authentication credential stored within the headers (Column 2, lines 18-35; and Column 7, lines 7-61).

Regarding Claim 19,

Lloyd discloses that the authentication modules comprise a set of dynamically extracted authentication parameters from service requests from the wireless clients (Column 7, lines 56-67), but does not disclose that this information is header information.

Liao, however, discloses that the service requests comprise headers, including information about the particular client (Column 2, lines 18-35; and Column 7, lines 7-61). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the wireless system headers of Liao into the authentication system of Lloyd in order to reduce the number of bits and bytes that must be transmitted over low bandwidth communication lines and to reduce the amount of memory used to store authentication information within each wireless client device (Column 2, lines 45-63).

Regarding Claim 20,

Lloyd as modified by Liao discloses the server of claim 19, in addition, Lloyd discloses that the authentication modules comprise selection logic to selectively choose authentication parameters in response to a client service request (Column 1, line 66 to Column 2, line 28; Column 6, line 34 to Column 7, line 10; and Figure 2).

Regarding Claim 21,

Lloyd as modified by Liao discloses the server of claim 20, in addition, Liao discloses that the client service request comprises HTTP request headers (Column 2, lines 18-35; and Column 7, lines 7-61).

Regarding Claim 22,

Lloyd as modified by Liao discloses the server of claim 21, in addition, Lloyd discloses that the authentication information comprises equipment manufacturer specified information (Column 11, lines 55-64), and Liao discloses that the authentication information is transmitted to the server in an authentication credential stored within the headers (Column 2, lines 18-35; and Column 7, lines 7-61).

Regarding Claim 23,

Lloyd as modified by Liao discloses the server of claim 22, in addition, Lloyd discloses programmable user specific information within the authentication information transmitted to the server (Column 7, lines 56-67), and Liao discloses that the authentication information is transmitted in an authentication credential stored within the headers (Column 2, lines 18-35; and Column 7, lines 7-61).

5. Claims 13, 14, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lloyd in view of iPlanet (Sun Microsystems, "iPlanet Portal Server Administrator Guide, Chapter 6 (Managing Authentication)", 5/4/2000, pp. 1-24, obtained from <http://docs.sun.com/source/816-6128-10/authctn.htm>), further in view of

Art Unit: 2137

Bloomberg (Bloomberg News, "Chips aim to make passwords obsolete", 12/31/1999, pp. 1-3, obtained from <http://news.com.com/2100-1040-235103.html>).

Regarding Claim 13,

Lloyd discloses that the plurality of authentication modules comprise:

A user identification module (Column 5, lines 41-64);

A password module (Column 5, lines 41-64);

A secureID module (which is secured) (Column 11, lines 55-64);

A Microsoft Windows/NT module (Column 6, lines 34-40);

But does not disclose a membership module, a safeword module, a S/key module, and a nopassword module.

iPlanet, however, discloses a membership module (Pages 1-2); a safeword module (Pages 1-2; and Pages 15-16); and a S/key module (Pages 1-2; and Pages 6-9). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication modules of iPlanet into the authentication system of Lloyd in order to give the system the ability to authenticate a broader range of wireless clients via additional authentication/support modules. iPlanet does not disclose a nopassword module.

Bloomberg, however, discloses a nopassword module (Pages 1-3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the biometrics system of Bloomberg

into the authentication system of Lloyd as modified by iPlanet in order to increase security and cut down on the cost of lost passwords.

Regarding Claim 14,

Lloyd as modified by iPlanet and Bloomberg discloses the system of claim 13, in addition, Lloyd discloses that the plurality of authentication modules further comprise:

A RADIUS authentication module (Column 5, line 65 to Column 6, line 5);

A UNIX authentication module (Column 6, lines 34-40); and

iPlanet discloses an LDAP authentication module (Pages 1-2; and Pages 9-11).

Regarding Claim 27,

Lloyd discloses that the plurality of authentication modules are presented to each of the plurality of classes of wireless clients (Column 1, line 66 to Column 2, line 28; Column 6, line 34 to Column 7, line 10; and Figure 2), but does not disclose that a URL is used to determine the plurality of authentication modules presented to each of the clients.

iPlanet, however, discloses that a URL is used to determine the plurality of authentication modules presented to each of the clients (Page 3, *How the Users Experience the Authentication Process*). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication modules of iPlanet into the

Art Unit: 2137

authentication system of Lloyd in order to give the system the ability to authenticate a broader range of wireless clients via additional authentication/support modules.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffrey D Popham
Examiner
Art Unit 2137


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER